AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☑ Original ☐ Duplicate

CLERK'S OFFICE
A TRUE COPY
Mar 15, 2023
s/ Erin Hayes
Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
A white Apple iPhone (MPD Inventory #23006928, Item #1) in the possession of the Milwaukee FBI Office, for a forensic examination of the SUBJECT DEVICE (See Attachments)

Case No. 23-m-333 (SCD)
Matter No.: 2023R00086

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 3-29-23 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Stephen C. Dries.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 3-15-23 1:30 pm

Stephen C. Dries
Judge's signature

City and state: Milwaukee, WI

Hon. Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A
Property to Search

The following property is to be searched:

a. A white Apple iPhone (MPD Inventory #23006928, Item #1) in evidence in a secured location at the FBI Office located in Eastern District of Wisconsin.

This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
Items to Seize

1. All records on the Devices described in Attachment A that relate to violations of Title 18, United States Code, Section 249, involving CORDELL M. HOWZE, which was in active memory of the SUBJECT DEVICE as of January 1, 2021, to include:

   a. any information related to possession of firearms (including photographs, text messages, emails, or any other communication information);

   b. any information regarding biases or hate regarding sexual orientation;

   c. any information recording the target's schedule or travel;

   d. any web search information related to the offenses described above;

   e. any communications via text messages, email, Facebook, Twitter, or other web-based applications between the subject and others regarding the offenses described above;

   f. any photographs or videos regarding the offenses described above; and

   g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage and any photographic form.

4. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A white Apple iPhone (MPD Inventory #23006928, Item #1) in the possession of the Milwaukee FBI Office, for a forensic examination of the SUBJECT DEVICE (See Attachments)

Case No. 23-m-333 (SCD)
Matter No.: 2023R00086

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C § 249	Hate Crime Acts;

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

SA Erin Lucker, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 3-15-23

_____
Judge's signature

City and state: Milwaukee, WI

Hon. Stephen C. Dries U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Erin Lucker, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of a white Apple iPhone in evidence in a secured location at the FBI Office located in Eastern District of Wisconsin, MPD Inventory #23006928, Item #1 ("SUBJECT DEVICE"), as described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent for the Federal Bureau of Investigation ("FBI"), where I have been employed since November 2016. I am currently assigned to an FBI squad which investigates civil rights crimes and public corruption crimes. I was previously assigned to the FBI Milwaukee Violent Crimes Task Force which involved investigations of violent crimes, to include kidnappings, extortions, murder for hire, and bank and armored car robberies. During my tenure with the FBI, I have participated in all aspects of investigations, including executing search warrants involving, among other things, the search and seizure of computers, computer equipment, software, and electronically stored information. Through my experience and training, I have become familiar with activities of individuals engaged in illegal activities, to include their techniques, methods, language, and terms. During my career, my investigations have included the use of various surveillance techniques and the execution of numerous search and seizure warrants, including for computers and cellular telephones.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies, all of whom I believe to be truthful and reliable. This affidavit is intended to show merely that there is sufficient

probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I submit that there is probable cause to believe that the SUBJECT DEVICE contain evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. 249 ("SUBJECT OFFENSES").

PROBABLE CAUSE

5. On Sunday, February 26, 2023, witness G.V. (DOB 9/20/1999) was sleeping at 5301 N. 29th Street, Apartment 7, Milwaukee, Wisconsin and woke up at approximately 5:33 a.m. after hearing a loud bang that could have been a gunshot. Between 8:15 a.m. and 8:30 a.m., G.V. smelled gas in the apartment and checked the stove to ensure there was not a gas leak. At approximately 9:15 a.m., G.V. observed light smoke in the apartment and contacted 911.

6. On Sunday, February 26, 2023, at approximately 9:21 a.m., Milwaukee Fire Department ("MFD") was dispatched to 5301 N. 29th Street, Milwaukee, Wisconsin, regarding a structure fire at that location. Upon arrival, MFD observed that Apartment 5 was on actively on fire and forced entry. After the fire was extinguished and the apartment was vented, MFD discovered a deceased victim, who was identified as C.H. (DOB 6/14/1991). C.H. was a transgender female who was assigned male at birth.

7. Milwaukee Police Department ("MPD") responded to the scene and conducted a scene investigation. Located in the residence was a red, plastic gas can with gasoline inside. In addition, one (1) 9mm cartridge was recovered in the bathroom of the residence. A red, 2019 Toyota Camry, Wisconsin license plate ARZ2792, registered to C.H., was recovered from the rear parking lot of 5301 N. 29th Street and towed to the City of Milwaukee Tow Lot for evidence processing.

8. A review of surveillance video captured an unidentified male (UM-1) walking south across the rear parking lot of 5277 S. 29th Street, Milwaukee, Wisconsin, at approximately 8:45 a.m. UM-1 continued behind the garage of 5266 N. Teutonia Avenue, Milwaukee, Wisconsin. Pole camera video then captured UM-1 walking on the driveway of 5262 N. Teutonia Avenue, Milwaukee, Wisconsin, and crossing Teutonia Avenue to the west side of the street. Additional pole camera video showed UM-1 walking south to Villard Avenue towards McDonalds, 5191 N. Teutonia Avenue, Milwaukee, Wisconsin, and then continuing to walk south on Teutonia Avenue, out of view of surveillance video and pole cameras.

9. In the surveillance and pole camera videos, UM-1 was observed wearing a black vest with a hood over a gray sweatshirt, light colored sweatpants with a dark colored stripe from the waist to the knees. UM-1 had glasses on top of his head and had his hair braided toward the back with short or shaved hair on the sides.

10. C.H.'s 2019 Toyota Camry was processed for evidence and latent prints were recovered from a Lysol wipes container located on the front passenger floorboard. An examination of the latent prints revealed a match to the left ring finger of CORDELL M. HOWZE (DOB 10/26/1989).

11. MPD officers interviewed P.S. (DOB 12/5/1996), who advised that HOWZE spent the night at P.S.'s home in Neenah, Wisconsin on Friday, February 24, 2023. On Saturday, February 25, 2023, P.S. gave HOWZE a ride to Milwaukee, Wisconsin, and dropped HOWZE off on 83rd Street at approximately 10:30 a.m. At this time, HOWZE was wearing light colored cargo pants and a dark jacket with grey sleeves. P.S. was shown surveillance still images of UM-1 from McDonalds, 5191 N. Teutonia Avenue, Milwaukee, Wisconsin. P.S. advised UM-1 looked like HOWZE, and the clothing UM-1 was wearing was consistent with clothes HOWZE was wearing when P.S. drove HOWZE to Milwaukee, Wisconsin, on Saturday, February 25, 2023.

12. On Monday, February 27, 2023, P.S.'s wife contacted P.S. and advised HOWZE was at their home in Neenah, Wisconsin. P.S. responded to his home and observed HOWZE in the living room with a black, red dot sight handgun with an extended magazine and green laser beam. HOWZE showed P.S. videos on HOWZE'S cell phone, which P.S. identified as HOWZE's white Apple iPhone. In the video, P.S. heard HOWZE'S voice, and in addition, P.S. recognized HOWZE'S face in the reflection of an aquarium. The video showed a deceased female wearing a t-shirt and underwear. There was an injury to the back of the female's head, and there was blood on the floor and pillows. In the video, HOWZE pointed a gun at an aquarium and pointed the green laser beam at a snake in the aquarium. P.S. observed that the video was shot on the second floor of a building. In addition, P.S. observed a yellow house through the window.

13. P.S.'s description of the video, to include the deceased woman, location of the injury, and the aquarium, was consistent with the February 26, 2023 crime scene at 5301 N. 29th Street, Apartment 5, Milwaukee, Wisconsin.

14. HOWZE told P.S. that HOWZE "caught a body of a disgusting ass transgender." HOWZE made comments that he wanted to kill a female that drove a red Dodge Caravan, and a male that kept contacting HOWZE about a vehicle HOWZE stole. At this time, P.S. told HOWZE to leave P.S.'s home. HOWZE sent P.S. the same video via text message from telephone number 414-581-2266. P.S. deleted the video because P.S. was disgusted by the content.

15. On February 28, 2023, HOWZE was observed exiting an apartment building in Neenah, Wisconsin, and entering a 2019 White Chevrolet Trax, Wisconsin license plate AEZ6823, registered to R.H. (DOB 1/12/1968), which is HOWZE's mother. City of Neenah Police Department ("NPD") Officers attempted to conduct a vehicle stop of HOWZE, but HOWZE continued to drive away. During the pursuit, officers observed HOWZE throw items from the

Chevrolet Trax, which included a blue Nike duffle bag; a clear, plastic bag containing unfired, 9mm cartridges; a black Sig Sauer P320 9mm semi-automatic handgun, serial number 58B229642, with a green laser attachment; and a white iPhone (SUBJECT DEVICE). After the pursuit, HOWZE was taken in to custody in Menasha, Wisconsin. The items thrown from the Chevrolet Trax were collected by law enforcement, including the white iPhone (SUBJECT DEVICE), which was placed in evidence at MPD under Inventory #23006928, Item #1. The FBI took custody of the SUBJECT DEVICE on March 2, 2023, which is now in a secured evidence area of the FBI Office in the Eastern District of Wisconsin. The SUBJECT DEVICE is believed to be the same white Apple iPhone that was used by HOWZE to show P.S. the video of the deceased woman.

16. On March 1, 2023, HOWZE'S mother, R.H., was interviewed by MPD detectives. R.H. advised she gave HOWZE a ride to Dunham's, 2550 S. 108th Street, West Allis, Wisconsin on Saturday, February 25, 2023, where HOWZE purchased a box of 9mm 100 gr FMJ lead ammunition. R.H. provided detectives with the receipt from Dunham's, which showed the purchase was made on February 25, 2023, at approximately 4:05 p.m. R.H. was aware that HOWZE possessed a handgun with a green laser.

17.R.H. was shown surveillance still images of UM-1 from the area of 5301 N. 29th Street, Milwaukee, Wisconsin. R.H. identified UM-1 as being HOWZE, and advised the clothing UM-1 wore was consistent with the clothing HOWZE wore when he left R.H.'s home on Saturday, February 25, 2023 and Sunday, February 26, 2023.

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored

images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate

the antenna's latitude, longitude, and sometimes altitude with a high level of precision

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

19. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at https://www.apple.com, I know that the SUBJECT DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by

a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

23. Manner of execution. Because this warrant seeks permission to examine a device that will already in law enforcement's possession, the execution of the search of the cellular device does not involve the further physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of this portion of the warrant at any time in the day or night.

Unlocking Electronic Devices Using Biometric Features

24. I know from my training and experience, as well as publicly available materials, that encryption systems for mobile phones and other electronic devices are becoming ever more widespread. Such encryption systems protect the contents of these devices from unauthorized access by users and render these contents unreadable to anyone who does not have the device's

password. As device encryption becomes more commonplace, the encryption systems implemented by device manufacturers are becoming more robust, with few—if any—workarounds available to law enforcement investigators.

25. I also know that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize. Therefore, I request that this warrant permit law enforcement agents to obtain from HOWZE the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that HOWZE's physical biometric characteristics will unlock the device(s).

26. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

27. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the

user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the frontfacing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

28. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

29. Access to the SUBJECT DEVICE may take longer than 14 days to process after the exam is started due to technology updates of forensic applications.

30. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

31. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices are subject to search and seizure pursuant to the applied-for warrant. The passcode

or password that would unlock such device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

32. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, certain Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. Due to the foregoing, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to obtain from HOWZE the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of the aforementioned person to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of the

aforementioned person to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

CONCLUSION

33. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT DEVICE described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A
Property to Search

The following property is to be searched:

a. A white Apple iPhone (MPD Inventory #23006928, Item #1) in evidence in a secured location at the FBI Office located in Eastern District of Wisconsin.

This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
Items to Seize

1. All records on the Devices described in Attachment A that relate to violations of Title 18, United States Code, Section 249, involving CORDELL M. HOWZE, which was in active memory of the SUBJECT DEVICE as of January 1, 2021, to include:

   a. any information related to possession of firearms (including photographs, text messages, emails, or any other communication information);

   b. any information regarding biases or hate regarding sexual orientation;

   c. any information recording the target's schedule or travel;

   d. any web search information related to the offenses described above;

   e. any communications via text messages, email, Facebook, Twitter, or other web-based applications between the subject and others regarding the offenses described above;

   f. any photographs or videos regarding the offenses described above; and

   g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage and any photographic form.

4. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.